Please type a plus sign (+) inside this box → +

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

03/24/99 C586 U.S. PTO

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1 53(b))

Attorney Docket No.	042390.P6526
First Inventor or Application Identifier	David A. Lee
Title	A Method and Apparatus for the Generation of Cryptographic Keys
Express Mail Label No.	EL123182074US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

JC542 U.S. PTO 09/275722 03/24/99

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. ☒ Specification [*Total Pages* 28]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (*if filed*)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. ☒ Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 10]

4. Oath or Declaration [*Total Pages* 3]
a. ☒ Newly executed (original copy)
b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d))
(for continuation/divisional with Box 16 completed)
☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR §§ 1.63(d)(2) and 1.33(b).

5. ☐ Microfiche Computer Program *(Appendix)*

6. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ☐ Computer Readable Copy
b. ☐ Paper Copy (identical to computer copy)
c. ☐ Statement verifying identity of above copies

**NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).*

ACCOMPANYING APPLICATION PARTS

7. ☒ Assignment Papers (cover sheet & document(s))
8. ☐ 37 C.F.R. § 3.73(b) Statement ☐ Power of Attorney
(when there is an assignee)
9. ☐ English Translation Document *(if applicable)*
10. ☐ Information Disclosure Statement (IDS)/PTO - 1449 ☐ Copies of IDS Citations
11. ☐ Preliminary Amendment
12. ☐ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
13. ☐ *Small Entity Statement(s) ☐ Statement filed in prior application, Status still proper and desired
14. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
15. ☐ Other: . . . . . .

16. If a **CONTINUING APPLICATION**, *check appropriate box, and supply the requisite information below and in a preliminary amendment:*
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: _____
Prior application Information: *Examiner* _____ *Group/Art Unit:* _____
For CONTINUATION or DIVISIONAL APPS only The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts

17. CORRESPONDENCE ADDRESS

☐ *Customer Number or Bar Code Label* *(Insert Customer No. or Attach bare code label here)* *or* ☒ *Correspondence address below*

Name	BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP				
Address	12400 Wilshire Boulevard, Seventh Floor				
City	Los Angeles	*State*	California	*Zip Code*	90025
Country	U.S.A.	*Telephone*	(714) 557-3800	*Fax*	(714) 557-3347

Name (Print/Type)	William W. Schaal, Reg. No. 39, 018		
Signature		*Date*	03/24/99

Burden Hour Statement: This form is estimated to take 0.2 hours to complete Time will vary depending upon the needs of the individual case Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

Docket No. 042390.P6526
Express Mail No.

UNITED STATES UTILITY PATENT APPLICATION

FOR

A METHOD AND APPARATUS FOR THE GENERATION OF CRYPTOGRAPHIC KEYS

Inventor:

David A. Lee

Prepared by:
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025-1026
(714) 557-3800

DRAFT - DO NOT COPY

BACKGROUND

1. FIELD

The invention relates to the field of data security. In particular, the present invention relates to a method and apparatus for generating cryptographic keys using a key matrix.

2. BACKGROUND ART

In today's society, it is becoming more and more desirable to transmit digital information from one location to another in a manner that is clear and unambiguous to a legitimate receiver, but incomprehensible to any illegitimate recipients. Accordingly, such information is typically encrypted using one of two commonly used cryptographic techniques: public key cryptography and symmetric key cryptography.

In symmetric key cryptography, a commonly possessed, symmetric key is used to encrypt and decrypt a message transmitted between a legitimate sender and a receiver. Such encryption and decryption is performed through well-known conventional algorithms such as Data Encryption Standard (DES). Although symmetric key cryptography is computationally simple, it relies on both parties maintaining the secrecy of the symmetric key. Also, the management of symmetric keys tends to be complex. Simply stated, if each sender needs a different symmetric key to communicate with each legitimate receiver, it is difficult, if not impossible, for use by businesses having a large number of employees. For example, in a business of 1000 employees, a maximum of 499,500 (1000×999/2) keys would need to be managed, provided that each employee is capable of communicating with any another employee within the business.

In general, public key cryptography involves the use of a public key and a private key (collectively referred to as a "key pair") which are two separate, but related keys. Normally, the public key is publicly available and widely used for encrypting a message directed to the owner of the key pair. The private key is maintained in confidence and usually is used for decryption of incoming encrypted message. As a result, public key cryptography tends to be more secure than symmetric key cryptography, but it is more cumbersome and computationally intensive. The intense computations tend to prevent consumer electronic devices and other lower performance devices from using public key cryptography.

Diffie-Hellman Key Exchange, a hybrid cryptographic technique developed in the late 1970s (U.S. Patent No. 4,200,770), allows two or more parties to exchange information over a public channel to form a secret that is known by all parties involved, but of which eavesdroppers cannot infer. While generation and use of the "secret" achieves the simplicity of symmetric key cryptography, its calculation is also computationally intensive. Diffie-Hellman involves the calculation of the secret through modular exponents over very large prime modular fields (e.g., 1024-bit binary numbers).

On or around 1985, elliptic curve cryptography (ECC) was proposed. ECC involves the translation of cryptographic techniques from modular exponentiation to scalar multiplication over an elliptic curve over a finite field. ECC helped alleviate the mathematical strain of performing these cryptographic calculations on smaller-sized integers to provide, in theory, a comparable level of security as that of the modular exponentiation over much larger-sized prime fields. However, this is only a partial performance improvement over modular exponentiation, and it also adds further to the complexity of implementation due to the extensive mathematical calculations involved.

In light of the foregoing, it would be desirable to develop a cryptographic technique that provides the security advantages of public key cryptography without the disadvantages of being cumbersome and computationally intensive. Furthermore, it would be desirable for the cryptographic technique to seamlessly work with revocation protocols to protect the system from reverse-engineering attacks.

Docket # P6526

SUMMARY OF THE INVENTION

Briefly, one embodiment of the invention is a method comprising providing a key matrix having N rows and M columns of matrix keys, where $N \geq 2$ and $M \geq 2$. For each column of the key matrix, arithmetic operations are performed on matrix keys of at least two selected rows of the key matrix to produce a first set of secret device keys. Then, a shared secret key is produced based on arithmetic operations on selected secret device keys of the first set of secret device keys.

Docket # P6526

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is an illustrative block diagram of an embodiment of a network featuring a certification authority dispensing keys produced from a key matrix.

Figure 2 is an illustrative block diagram of the certification authority of the network of Figure 1.

Figure 3 is an illustrative block diagram of a first embodiment of a two-dimensional key matrix.

Figure 4 is an illustrative block diagram of a first secret device key set and a key selection vector provided to the first digital platform using the key matrix of Figure 3.

Figure 5 is an illustrative block diagram of a second secret device key set and a key selection vector provided to the second digital platform using the key matrix of Figure 3.

Figure 6 is an illustrative block diagram of a second embodiment of a two-dimensional key matrix.

Figure 7 is an illustrative block diagram of a first secret device key set and a key selection vector provided to the first digital platform using the key matrix of Figure 6.

Figure 8 is an illustrative block diagram of a second secret device key set and a key selection vector provided to the second digital platform using the key matrix of Figure 6.

Figure 9 is an illustrative block diagram of a third embodiment of a two-dimensional key matrix.

Figure 10 is an illustrative block diagram of a first secret device key set provided to the first digital platform using the key matrix of Figure 9.

Figure 11 is an illustrative block diagram of a second secret device key set provided to the first digital platform using the key matrix of Figure 9.

Figure 12 is an illustrative block diagram of a secret device key set provided to the second digital platform acting as an information receiver using the key matrix of Figure 9.

Figure 13 is an illustrative block diagram of an alternate secret device key set provided to the second digital platform acting as an information provider using the key matrix of Figure 9.

Figure 14 is an illustrative block diagram of a matrix authentication scheme with revocation between the first digital platform and the second digital platform of Figure 1.

Figure 15 is an illustrative block diagram of a matrix authentication scheme without revocation between the first digital platform and the second digital platform of Figure 1.

DETAILED DESCRIPTION

In brief, the present invention relates to a system and method for generating cryptographic keys using a key matrix. In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be obvious to one skilled in the art, however, that the present invention may be practiced without these specific details.

To clarify various characteristics and features of the present invention, certain terminology is used. For example, a "digital platform" is defined as any hardware with processing and internal data storage capabilities. Examples of digital platforms include, but are not limited or restricted to the following: computers (e.g., laptops, desktops, hand-helds, servers, mainframes, etc.), imaging equipment (e.g., printers, facsimile machines, scanners, digital cameras, etc.), set-top boxes (e.g., television control boxes for cable or satellite transmissions), wireless communication equipment (e.g., cellular phones, pagers, etc.), consumer electronic appliances and the like. A "channel" is generally defined as one or more pathways through which information may be transferred (directly, indirectly or broadcast) over information-carrying mediums such as, for example, electrical wire, fiber optic, cable, bus, plain old telephone system (POTS) line, wireless (e.g., satellite, radio frequency "RF", infrared, etc.) or even a logical link. "Information" is defined as data, address, control or any combination thereof.

With respect to cryptography related terminology, the term "secure" indicates a state where it is not reasonably feasible for an unauthorized individual to access information in an non-encrypted format. A "key" is generally defined as an encoding and/or decoding parameter usually structured as a sequence of binary data. A "digital signature" includes digital information signed with a private key of its signatory to ensure that the digital information has not been illicitly modified after being digitally signed.

This digital information may be provided in its entirety or as a digest produced by a one-way hash function. The "one-way hash function" includes a function, mathematical or otherwise, that converts information from a variable-length to a fixed-length (referred to as a "digest"). The term "one-way" indicates that there does not readily exist an inverse function to recover any discernible portion of the original information from the fixed-length digest. Examples of a hash function include MD2 or MD5 provided by RSA Data Security of Redwood City, California, or Secure Hash Algorithm (SHA-1) as specified by the National Institute of Standards and Technology located in Washington, D.C.

In addition, a "digital certificate" includes digital information used to authenticate a sender of information. For example, a digital certificate may include information concerning a person, entity or device being certified that is encrypted with the private key of a certification authority. Examples of a "certification authority" include an original equipment manufacturer (OEM), a software vendor, a trade association, a governmental entity, a bank or any other trusted business or person.

Referring now to Figure 1, an illustrative block diagram of an embodiment of a network 100 employing at least two digital platforms is shown. Network 100 includes a first digital platform 120 and a second digital platform 130 capable of establishing communications with certification authority 110 via channels 140 and 150, respectively. Platforms 120 and 130 can register with certification authority 110 in order to receive secret device keys therefrom. Each platform 120 or 130 can be classified as either (i) an information provider, or (ii) an information receiver, or (iii) a transceiver capable of operating as either an information provider or an information receiver. Of course, other classification schemes may be utilized so long as communicative platforms have compatible classifications. Also, first and second digital platforms 120 and 130 communicate with each other via channel 160.

As shown in Figure 2, an embodiment of certification authority 110 is shown. Certification authority 110 comprises a digital platform that includes a processing unit 200 and memory 210. In particular, processing unit 200 is any hardware having code processing capabilities such as, for example, a central processing unit, a microcontroller, a coprocessor, a state machine and the like. Processing unit 200 accesses information from memory 210. In one embodiment, memory 210 is volatile memory with data backed-up in non-volatile storage. Of course, it is contemplated that memory 210 may be implemented to operate as non-volatile memory to ensure that its contents are retained during a power-down condition. Thus, memory 210 may include, for example, (i) read only memory (ROM), (ii) any type of programmable read only memory (PROM) such as erasable PROM (EPROM) or electrically erasable PROM (EEPROM), (iii) flash memory, or even (iv) battery-backed volatile memory.

Memory 210 retains the certification authority's public key (PUKCA) 220, its private key (PRKCA) 230, and a multi-dimensional matrix 240 of matrix keys (K) arranged in grids (e.g., rows, columns, along z-axis, etc.) held in secret to be known only by certification authority 110 of Figure 1. PUKCA 220 and PRKCA 230 are provided to support matrix key authentication schemes, not the formation of shared secret key "SECKEY". Currently, each key is 64-bits, although any bit size may be used (e.g., 32, 128, 160, 256, 512, 1024...). For increased protection, PRKCA 230 and key matrix 240 may be obfuscated by tamper-resistant software. The dimensions of key matrix 240 and length of the matrix keys correspond to the desired strength of security for network 100 of Figure 1.

In the event that key matrix 240 is a two-dimensional n×m matrix, for example, one matrix dimension (e.g., "n" rows) may be assigned to a first platform classification while the other matrix dimension (e.g., "m" columns) is assigned to a second platform classification. The "platform classifications" need only be something that can

differentiate participants of the authentication. Thus, the classification may be (1) information provider/information receiver; (2) multiple types of information providers; and (3) multiple types of information receivers and the like. Thus, if the first platform classification is an information provider, it would receive "m" secret device key sets created by performing arithmetic operations on the matrix keys situated in selected "p" rows ($p<n$) for each column. For this embodiment, the arithmetic operation involves modular addition, although exclusive-or (XOR) operations, non-modular addition or other operations may be used. Information receivers (second class), however, would receive "n" secret device key sets created by performing arithmetic operations on the matrix keys situated in selected "q" columns ($q<m$) for each row. For maximum security, "p" is equal to $\frac{n}{2}$ and "q" is equal to $\frac{m}{2}$; however, p or q may be any selected number of rows or columns less than n or m, respectively (see Figure 6).

Referring now to Figure 3, an illustrative block diagram of a first embodiment of key matrix 240 is shown. Key matrix 240 is a two-dimensional, n×m matrix with a first dimension (e.g., rows) 300 dedicated to a first platform classification (e.g., an "information provider" class) and a second dimension (e.g., columns) 310 dedicated to a second platform classification (e.g., an "information receiver" class). For clarity sake, key matrix 240 is represented as a 6×6 matrix; however, key matrix 240 normally comprises a larger-sized matrix, even a 40×40 matrix or larger. It is contemplated that the dedication of matrix dimensions for each class could be different. For example, columns and rows could be dedicated to the "information provider" and "information receiver" classes, respectively.

For each digital platform, the certification authority generates a combination of rows or columns associated with key matrix 240. Preferably, the combination is unique, but uniqueness is not required. For example, in this embodiment, if the first digital platform is classified as an information provider, the certification authority generates a

combination of rows, which is represented as a first key selection vector (KSV1) 320 for the first digital platform. Herein, KSV1 320 is equal to <2, 3, 5>. Based on KSV1 320, the certification authority generates a set of secret device keys (1_SDKEY1 - 1_SDKEY6) 330-335 and provides both KSV1 320 and the first set of secret device keys 330-335 to the first digital platform. As shown in Figure 4, secret device keys 330-335 are generated through modular addition (e.g., modulo 2^{64}) of matrix keys in the selected rows of key matrix 240 for each column.

Referring back to Figure 3, if the second digital platform is classified as an information receiver, the certification authority generates a combination of columns associated with key matrix 240, which is represented as a second key selection vector (KSV2) 340. Herein, KSV2 340 is equal to <1, 3, 4>. Based on KSV2 340, certification authority generates a set of secret device keys (2_SDKEY1 - 2_SDKEY6) 350-355 and provides both KSV2 340 and the set of secret device keys 350-355 to the second digital platform. As shown in Figure 5, for each row, the second set of secret device keys 350-355 are produced through modular addition of the matrix keys of key matrix 240 pertaining to those columns selected by KSV2 340.

To secure channel 160 of Figure 1, the first and second digital platforms exchange KSV1 320 and KSV2 340. Hence, based on KSV2 340, the first digital platform creates a shared secret key (SECKEY) equivalent to the modular addition of 1_SDKEY1, 1_SDKEY3 and 1_SDKEY4. Concurrently, based on KSV1 320, the second digital platform also produces SECKEY through modular addition of 2_SDKEY2, 2_SDKEY3 and 2_SDKEY5. As shown in equation (1), SECKEY is determined to be the following:

$$(1)\quad \text{SECKEY (at DP1)} = (K21+K31+K51)+(K23+K33+K53)+(K24+K34+K54)$$
$$= (K21+K23+K24)+(K31+K33+K34)+(K51+K53+K54)$$

Referring now to Figure 6, an illustrative block diagram of a second embodiment of key matrix 240 is shown. Key matrix 240 is a two-dimensional, n×m matrix with a first dimension (e.g., rows) 400 dedicated to the "information provider" class and a second dimension (e.g., columns) 410 dedicated to the "information receiver" class. For clarity sake, key matrix 240 is represented as a rectangular (4×5) matrix in lieu of a square (6×6) matrix as shown in Figure 3.

Similarly, before providing keys to a digital platform, the certification authority generates a key selection vectors for that digital platform. For example, if the first digital platform is classified as an information provider, the certification authority generates a first key selection vector (KSV1) 420 to identify the selected combination of rows. Herein, KSV1 420 is equal to <2, 3> for example. Based on KSV1 420, certification authority generates a set of secret device keys (1_SDKEY1 - 1_SDKEY5) 430-434 and provides both KSV1 420 and a first set of secret device keys 430-434 to the first digital platform. As shown in Figure 7, secret device keys 430-434 are generated through modular addition on matrix keys in key matrix 240 that are associated with the rows selected by KSV1 420.

Referring back to Figure 6, if the second digital platform is classified as an information receiver, the certification authority generates a combination of columns stored in a second key selection vector (KSV2) 440. Herein, KSV2 440 is equal to <2, 3>. Based on KSV2 440, certification authority generates a second set of secret device keys (2_SDKEY1 - 2_SDKEY4) 450-453 and provides both KSV2 440 and secret device keys 450-453 to the second digital platform. Only four (4) secret device keys 450-453 are provided in this example because key matrix 240 features four rows. As shown in Figure 8, secret device keys 450-453 are produced through modular addition of the matrix keys of key matrix 240 for those columns selected by KSV2 440.

To generate SECKEY, the first and second digital platforms still exchange KSV1 420 and KSV2 440. Hence, based on KSV2 440, the first digital platform creates SECKEY equivalent to the modular addition of 1_SDKEY2 and 1_SDKEY3. Based on KSV1 420, the second digital platform generates SECKEY through modular addition of 2_SDKEY2 and 2_SDKEY3. As a result, as shown in equation (2), SECKEY is calculated to be the following:

(2) K22+K32+K23+K33 = SECKEY= K22+K23+K32+K33

Referring now to Figure 9, an illustrative block diagram of a third embodiment of key matrix 240 is shown. Key matrix 240 is a two-dimensional, n×m matrix with a first dimension (e.g., rows) 500 dedicated to the "information provider" class and a second dimension (e.g., columns) 510 dedicated to the "information receiver" class. For clarity sake, key matrix 240 is symmetric and represented as a 4×4 matrix.

Before providing keys into a digital platform, the certification authority generates key selection vectors for that digital platform. Likewise, these vectors may be unique to achieve better security. Since first digital platform is a transceiver in this embodiment, it would be required to store two sets of secret device keys. One set would be used when the first digital platform is functioning as an information provider and the other set would be used when functioning as an information receiver. In this embodiment, the certification authority assigns a first key selection vector (KSV1) 520, equal to <2, 3> when the first digital platform is functioning as an information provider. Also, the certification authority assigns a second key selection vector (KSV2) 540, equal to <2,4>, when the first digital platform functions as an information receiver. Of course, KSV1 and KSV2 may be equivalent for simplicity.

Based on KSV1 520, the certification authority generates a set of secret device keys (1_SDKEY1 - 1_SDKEY4) 530-533 and provides both KSV1 520 and secret device

keys 530-533 to the first digital platform. As shown in Figure 10, the set of secret device keys 530-533 are produced through modular addition on the matrix keys of key matrix 240 for rows selected by KSV1 520.

Based on KSV2 540, the certification authority also produces a set of secret device keys (1_SDKEY5 - 1_SDKEY8) 550-553 and provides both KSV2 540 and secret device key sets 550-553 to the first digital platform for use when acting as an information receiver. As shown in Figure 11, secret device keys 550-553 are generated through modular addition on the matrix keys of key matrix 240 for columns selected by KSV2 540.

Thereafter, if the second digital platform is classified as an information receiver, the certification authority generates a third key selection vector (KSV3) 560. Herein, KSV3 560 is equal to <2, 3>. Based on KSV3 560, the certification authority generates a set of secret device keys (2_SDKEY1 - 2_SDKEY4) 570-573 and provides both KSV3 560 and secret device keys 570-573 to the second digital platform. As shown in Figure 12, secret device keys 570-573 are produced through modular addition on the matrix keys of key matrix 240 for columns selected by KSV3 560.

To generate SECKEY, KSV1 520 and KSV3 560 are exchanged between the first and second digital platforms. Hence, based on KSV3 560, the first digital platform creates a shared secret key (SECKEY) equivalent to the modular addition of 1_SDKEY2 and 1_SDKEY3. Based on KSV1 520, the second digital platform generates SECKEY through modular addition of 2_SDKEY2 and 2_SDKEY3, where SECKEY is determined as follows:

$$K22+K32+K23+K33 = SECKEY = K22+K23+K32+K33$$

If the second digital platform is alternatively classified as an information provider as shown by dashed lines, the certification authority would have generated a fourth key selection vector (KSV4) 580. Herein, KSV4 580 is equal to <2, 3>. Based on KSV4 580, certification authority generates a set of secret device keys (2_SDKEY5 - 2_SDKEY8) 590-593 and provides both KSV4 580 and secret device keys 590-593 to the second digital platform. As shown in Figure 13, secret device keys 590-593 are generated by performing modular addition on the matrix keys of key matrix 240 for columns selected by KSV4 580.

To generate the shared secret key for providing a secure channel, KSV2 540 and KSV4 580 are exchanged between the first and second digital platforms. Hence, based on KSV4 580, the first digital platform creates a shared secret key (SECKEY) equivalent to the modular addition of 1_SDKEY6 and 1_SDKEY7. Based on KSV2 540, the second digital platform generates SECKEY through modular addition of 2_SDKEY6 and 2_SDKEY8. The SECKEY is determined as follows:

$$K22+K24+K32+K34 = SECKEY = K22+K32+K24+K34$$

Referring back to Figure 1, when digital platforms 120 and 130 are in compatible classes (e.g., one platform functioning as an information provider while the other platform functioning as an information receiver) and decide to inter-operate, both digital platforms 120 and 130 undergo a matrix authentication scheme, namely either a matrix authentication with revocation (see Figure 14) or a matrix authentication without revocation (see Figure 15). During the matrix authentication scheme, various secret device key sets of each digital platform 120 and 130 are used produce a shared secret key used to secure channel 160.

Referring now to Figure 14, an illustrative embodiment of a matrix authentication with revocation scheme between first digital platform 120 and second digital platform

130 is shown. In this embodiment, first digital platform 120 sends an authentication request 600 to second digital platform 130. Authentication request 600 comprises a random number (R1) 610, a digital certificate (CERT1) 620 and a key selection vector associated with first digital platform (KSV1) 630. KSV1 630 comprises information to indicate the combination of rows or columns selected for first digital platform 120. R1 610 is a random number used to prevent replay. In this embodiment, CERT1 620 comprises KSV1 630, a device identification (DEVID) 640 and possibly other values for first digital platform and a digital signature 650, all of which certified by PRKCA 220. Digital signature 650 comprises a hash result 660 of KSV1 630 and DEVID 640 after undergoing a one-way hash function and the hash result 660 being digitally signed with PRKCA 220.

Upon receiving authentication request 600, second digital platform 130 authenticates first digital platform 120 by recovering KSV1 630, DEVID 640 and digital signature 650 because PUKCA 220 is widely available. DEVID 640 is used by second digital platform 130 to determine whether first digital platform 120 is authorized to communicate in a secure fashion with second digital platform 130 by checking the revocation list. If so, KEY1 670 is generated based on KSV1 630 provided by first digital platform 120. If not, the authentication request is ignored.

Thereafter, second digital platform 130 provides a random number (R2) 680 and its selection vector (KSV2) 690 to first digital platform 120. From that, first digital platform 120 creates KEY2 700 and a check hash value (CV) 710. CV 710 is equivalent to a hash operation performed on the concatenation of KEY2 700, R1 610 and R2 680. CV 710 is provided to second digital platform 130 and compared with a resultant value of a hash of KEY1 670, R1 610 and R2 680. If CV 710 matches the resultant hash value, both KEY1 and KEY2 670 and 680 are identical and used as a shared secret key.

Alternatively, identical portions of KEY1 and KEY2 670 and 680 may be used as the shared secret key or even the hash result itself.

Of course, this is an illustrative example of the matrix authentication scheme. The matrix authentication scheme may be devised without the use of digital signatures.

Referring to Figure 15, an illustrative embodiment of a matrix authentication scheme without revocation between first digital platform 120 and second digital platform 130 is shown. In this embodiment, first digital platform 120 sends authentication request 800 to second digital platform 130. Authentication request 800 comprises a random number (R1) 810, and a key selection vector associated with first digital platform (KSV1) 830. KEY1 840 is calculated based on KSV1 830 provided by first digital platform 120.

Thereafter, second digital platform 130 provides a random number (R2) 850 and its selection vector (KSV2) 860 to first digital platform 120. From that, first digital platform 120 creates KEY2 870 and a check hash value (CV) 880. CV 880 is equivalent to a hash operation performed on the modular addition result of KEY2 870, R1 810 and R2 850. CV 880 is provided to second digital platform 130 and compared with a resultant value of a hash of KEY1 840, R1 810 and R2 850. If CV 880 matches the hash result, both KEY1 and KEY2 840 and 870 are identical. Thus, these keys 840 and 870 or portions thereof may be used as the shared secret key (SECKEY). Also, KEY1 and KEY2 may be used in combination with other data in possession by both digital platforms to produce SECKEY.

It is contemplated that matrix key authentication is not limited to simply two parties. It is possible to use matrix key authorization simultaneously between three or more parties. This is accomplished by extending the dimensions of the key matrix held by the certification authority for each additional party, and the dimensions of the number of matrix keys given to the various participants.

For example, in a three-way authentication scheme, a three-dimensional (3D) key matrix is needed where the matrix dimensions do not have to be equal. The 3D key matrix supports three "classes" of digital platforms, which we will refer to as Class 1, Class 2 and Class 3. These classes need only be something that can be differentiated between the participants of the authentication. Some examples might be (1) information source / intermediate information filter / information receiver; (2) information source for information type A, information source for information type B, information receiver; (3) authentication initiator, next device found to authenticate, third device to authenticate; (4) lowest device identification number, middle device identification number, highest device identification number, etc. The digital platforms receive secret device key sets for each class they might belong to.

In this embodiment, a 4×6×8 key matrix of 192 keys is provided. The first dimension is of size 4 and is for Class 1. The second dimension is of size 6 and is for Class 2. The third dimension is of size 8 and is for Class 3. For clarity sake, matrix keys are labeled "$K_{xyz,}$" where the first subscript (x) is the index of the first dimension, the second subscript (y) is the index of the second dimension, and the third subscript (z) is the index of the third dimension (Class 3).

Platform A is of Class 1 and is assigned combination <2,3>. It receives a 6×8 matrix of keys A_{yz}, where $A_{yz} = K_{2yz} + K_{3yz}$.

Platform B is of Class 2 and is assigned combination <3,5,6>. It receives a 4×8 matrix of keys B_{xz}, where $B_{xz} = K_{x3z} + K_{x5z} + K_{x6z}$.

Platform C is of Class 3 and is assigned combination <1,4,5,7>. It receives a 4×6 matrix of keys C_{xy}, where $C_{xy} = K_{xy1} + K_{xy4} + K_{xy5} + K_{xy7}$.

During authentication, the three digital platforms provide each other with their respective key selection vectors, and they subsequently combine their keys along the dimensions associated with the other platforms' key selection vectors.

Platform A receives key selection vector <3,5,6> from platform B (corresponding to the first dimension of platform A's secret device key set), and key selection vector <1,4,5,7> from platform C (corresponding to the second dimension of its secret A keys). Platform A then performs arithmetic operations on its secret device key sets (A_{yz}) for y = 3,5,6 and z = 1,4,5,7 to calculate the shared secret key (SECKEY) from the following:

$A_{31} + A_{34} + A_{35} + A_{37} + A_{51} + A_{54} + A_{55} + A_{57} + A_{61} + A_{64} + A_{65} + A_{67} = (K_{231} + K_{331}) + (K_{234} + K_{334}) + (K_{235} + K_{335}) + (K_{237} + K_{337}) + (K_{251} + K_{351}) + (K_{254} + K_{354}) + (K_{255} + K_{355}) + (K_{257} + K_{357}) + (K_{261} + K_{361}) + (K_{264} + K_{364}) + (K_{265} + K_{365}) + (K_{267} + K_{367})$. This is the sum of all K_{ijk} for $i = 2,3$; $j = 3,5,6$; and $k = 1,4,5,7$.

Platform B receives key selection vector <2,3> from platform A and key selection vector <1,4,5,7> from platform C. Platform B then performs arithmetic operations on its secret device key sets (B_{xz}) for x = 2,3 and z = 1,4,5,7 to calculate the following: $B_{21} + B_{24} + B_{25} + B_{27} + B_{31} + B_{34} + B_{35} + B_{37}$. This is also equal to the sum of all K_{ijk} for $i = 2,3$; $j = 3,4,5$; and $k = 1,4,5,7$.

Platform C receives key selection vector <2,3> from platform A and key selection vector <3,5,6> from platform B. Platform C then performs arithmetic operations on its secret device key sets (C_{xy}) for x = 2,3 and y = 3,5,6 to calculate the following: $C_{23} + C_{25} + C_{26} + C_{33} + C_{35} + C_{36}$. This is also equal to the sum of all K_{ijk} for $i = 2,3$; $j = 3,5,6$; and $k = 1,4,5,7$.

The three digital platforms have each calculated a shared secret value that they all agree upon. An eavesdropper cannot calculate SECKEY without knowing the secret

device key set of at least one of the respective devices. An interloper cannot emulate one of the three platforms to participate in this shared secret key formation without having available a set of secret device keys of the class it is emulating derived for the same key matrix kept secret by the certification authority.

Of course, the invention described herein may be designed in many different methods and using many different key manipulation schemes or circuitry. While the present invention has been described in terms of various embodiments to facilitate understanding of the present invention, other embodiments may come to mind to those skilled in the art without departing from the spirit and scope of the present invention. The invention should, therefore, be measured in terms of the claims that follow.

CLAIMS

What is claimed is:

1. A method comprising:

providing a key matrix having N rows and M columns of matrix keys, where $N \geq 2$ and $M \geq 2$;

for each column of the key matrix, performing arithmetic operations on matrix keys of at least two selected rows of the key matrix to produce a first set of secret device keys;

producing a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys.

2. The method of claim 1, wherein the arithmetic operations include modular addition.

3. The method of claim 1, wherein prior to performing the arithmetic operations, the method comprises:

generating a key selection vector identifying the at least two selected rows of the key matrix from which to produce the first set of secret device keys.

4. The method of claim 3, wherein the key selection vector is uniquely assigned to a first digital platform.

5. The method of claim 4, wherein prior to producing the shared secret key, the method comprises:

receiving a key selection vector from a second digital platform in communication with the first digital platform; and

analyzing contents of the key selection vector from the second digital platform to determine the selected secret device keys of the first set of secret device keys.

6. The method of claim 1, wherein prior to performing arithmetic operations on keys of at least two selected rows, the method further comprises:

dedicating the rows of the key matrix to a first classification; and

dedicating the columns of the key matrix to a second classification.

7. The method of claim 6, wherein the first classification includes digital platforms designed to provide information to other digital platforms.

8. The method of claim 7, wherein the second classification includes digital platforms designed to receive information from other digital platforms.

9. The method of claim 1, wherein the producing of the shared secret key comprises:

analyzing contents of an incoming key selection vector; and

performing arithmetic operations of the selected secret device keys located in columns of the key matrix identified by the contents of the incoming key selection vector.

10. The method of claim 9, wherein the producing of the shared secret key further comprises:

performing a hash operation on results of the arithmetic operations of the selected secret device keys located in the column of the key matrix identified by the contents of the incoming key selection vector.

11. A method comprising:

providing a key matrix having N rows and M columns of matrix keys, where N≥2 and M≥2;

for each row of the key matrix, performing arithmetic operations on matrix keys of at least two selected columns of the key matrix to produce a first set of secret device keys;

producing a shared secret key based on arithmetic operations on selected secret device keys of the first set of secret device keys.

12. The method of claim 11, wherein the arithmetic operations include modular addition.

13. The method of claim 11, wherein prior to performing the arithmetic operations, the method comprises:

generating a key selection vector identifying the at least two selected rows of the key matrix from which to produce the first set of secret device keys.

14. The method of claim 13, wherein the key selection vector is uniquely assigned to a first digital platform.

15. The method of claim 14, wherein prior to producing the shared secret key, the method comprises:

receiving a key selection vector from a second digital platform in communication with the first digital platform; and

analyzing contents of the key selection vector from the second digital platform to determine the selected secret device keys of the first set of secret device keys.

16. The method of claim 1, wherein prior to performing arithmetic operations on keys of at least two selected columns, the method further comprises:

dedicating the rows of the key matrix to a first classification; and

dedicating the columns of the key matrix to a second classification.

17. The method of claim 11, wherein the producing of the shared secret key comprises:

analyzing contents of an incoming key selection vector; and

performing arithmetic operations of the selected secret device keys located in rows of the key matrix identified by the contents of the incoming key selection vector.

18. The method of claim 17, wherein the producing of the shared secret key further comprises:

performing a hash operation on results of the arithmetic operations of the selected secret device keys located in the rows of the key matrix identified by the contents of the incoming key selection vector.

19. A machine readable medium having embodied thereon a computer program for processing by a first digital platform including memory containing the computer program comprising:

an authentication function to recover an incoming key selection vector and to compute a shared secret key based on a set of secret device keys stored in the first digital platform and the contents of the incoming key selection vector;

a transfer function to output at least a key selection vector assigned to the first digital platform;

a hash function to perform a hash operation on at least the shared secret key to produce a resultant hash value; and

a comparison function to compare the resultant hash value with an incoming check hash value received subsequent to the transmission of the key selection vector.

20. A network comprising:

a first digital platform; and

a certification authority in communication with the first digital platform, the certification authority having access to a key matrix featuring matrix keys arranged in accordance with at least a first dimension and a second dimension, generating a first key selection vector and providing a first set of secret device keys produced from selected matrix keys of the key matrix.

21. The network of claim 20 further comprising:

a second digital platform in communication with the certification authority and the first digital platform, the second digital platform being uniquely assigned a second key selection vector indicating at least two grids of the key matrix and a second set of secret device keys produced from matrix keys situated in at least two grids of the key matrix.

22. The network of claim 21, wherein the first and second digital platforms to exchange the first and second key selection vectors in order for each digital platform to produce a shared secret key to ensure that communications between the first and second digital platforms are secure.

23. A certification authority comprising:

a memory to store a key matrix having N rows and M columns of matrix keys, where $N \geq 2$ and $M \geq 2$;

a logic to generate a key selection vector for each digital platform registered with the certification authority.

24. The certification authority of claim 23, wherein the logic includes a processing unit.

25. The certification authority of claim 24, wherein the processing unit produces a first set of secret device keys by performing arithmetic operations on matrix keys along selected columns of the key matrix identified by the key selection vector to provide a first set of secret device keys to a digital platform.

26. The certification authority of claim 25, wherein the matrix keys along the processing unit performs arithmetic operations on matrix keys along selected rows of the key matrix identified by the key selection vector to provide a first set of secret device keys to a digital platform.

27. The certification authority of claim 23, wherein the matrix keys are only known by the certification authority.

ABSTRACT OF THE INVENTION

A method for formation of a shared secret key using a key matrix and a corresponding authentication protocol are described. The shared secret key formation scheme is a method in which sets of secret device keys are formed from arithmetic operations on matrix keys of a key matrix. The contents of the key matrix are held in confidence by the certification authority. The selection of which matrix keys to use is based on a key selection vector assigned by the certification authority. From the secret device keys, a shared secret key may be formed in accordance with a selected authentication protocol.

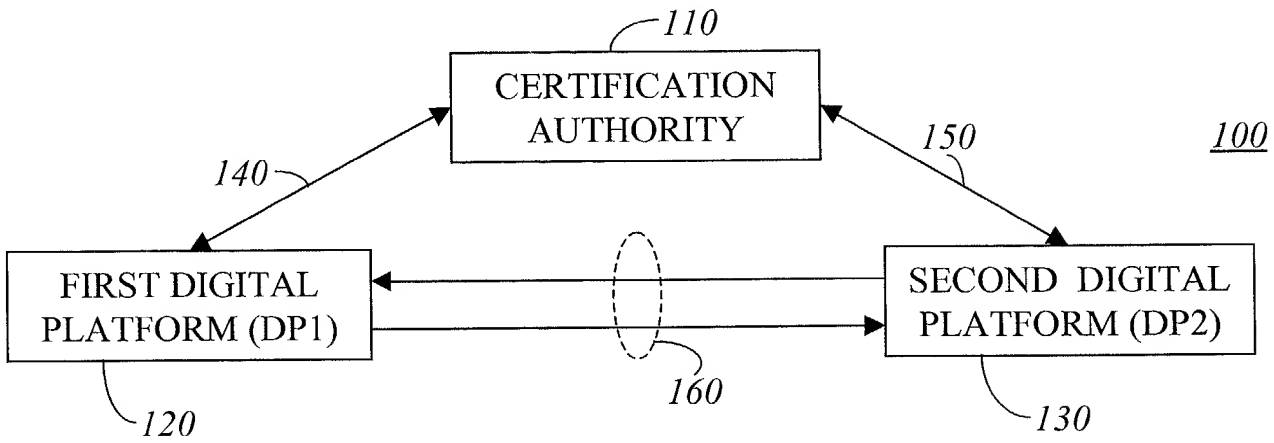


Figure 1

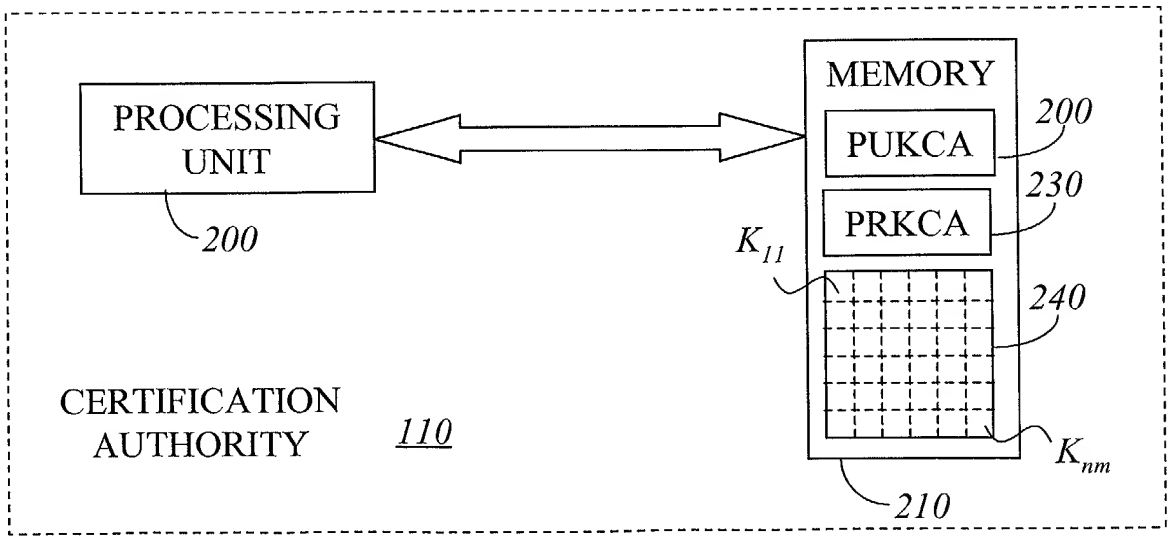


Figure 2

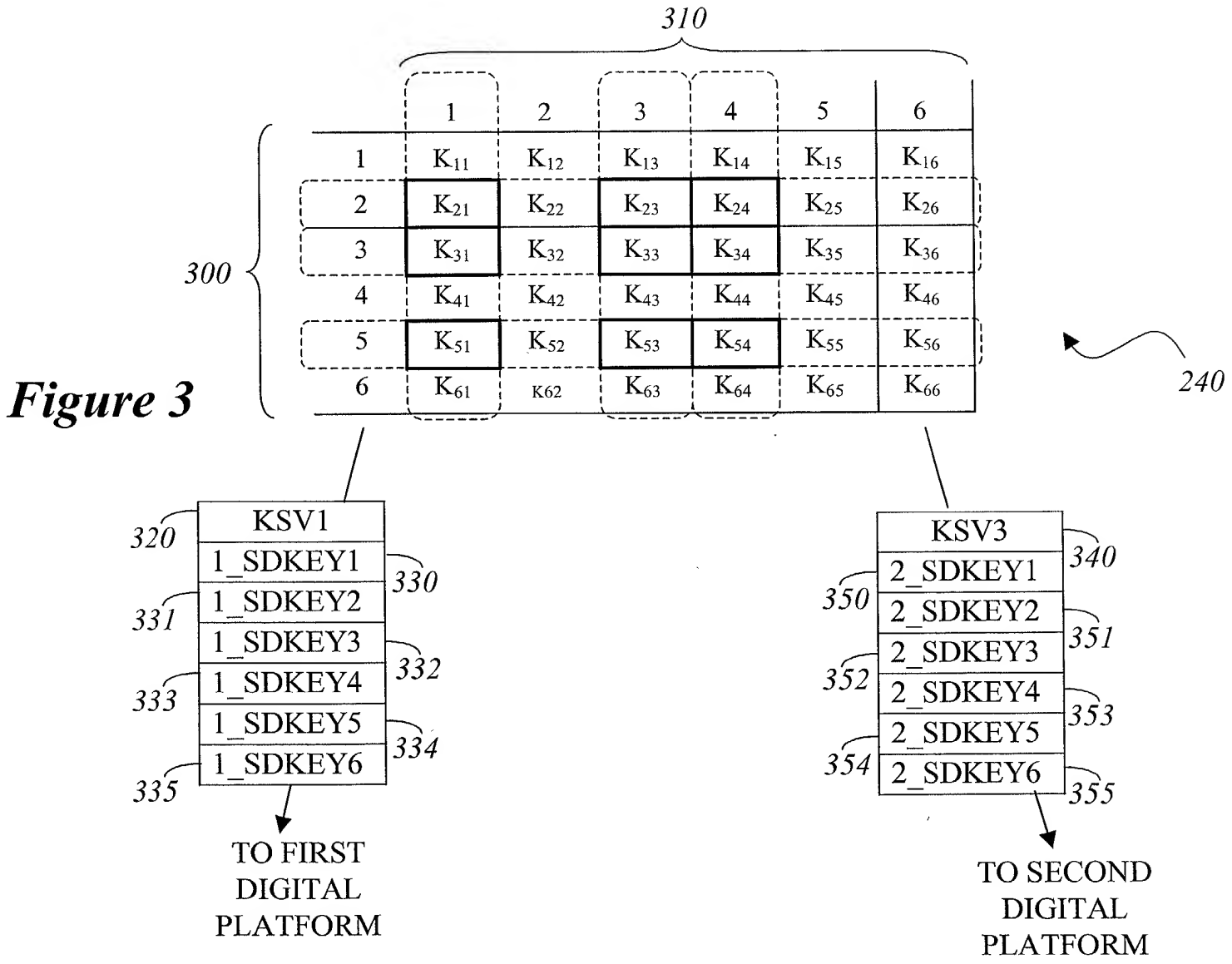
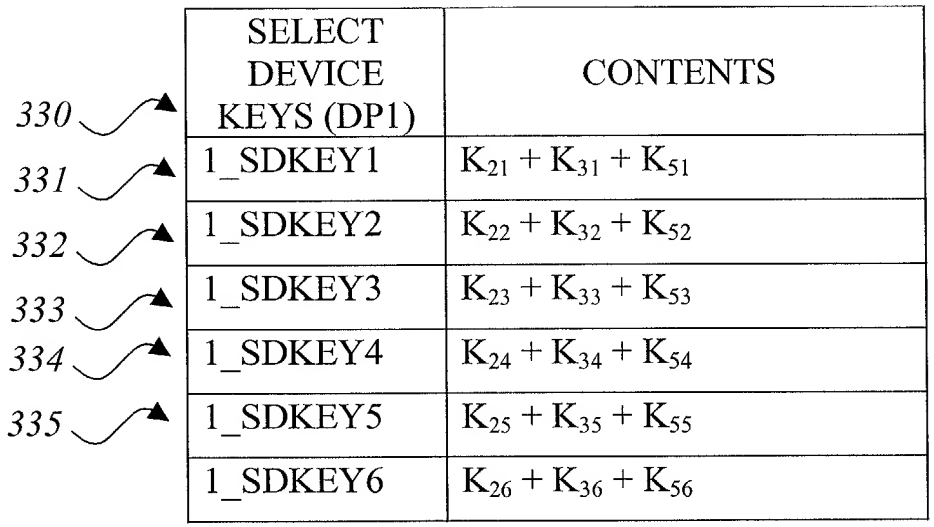
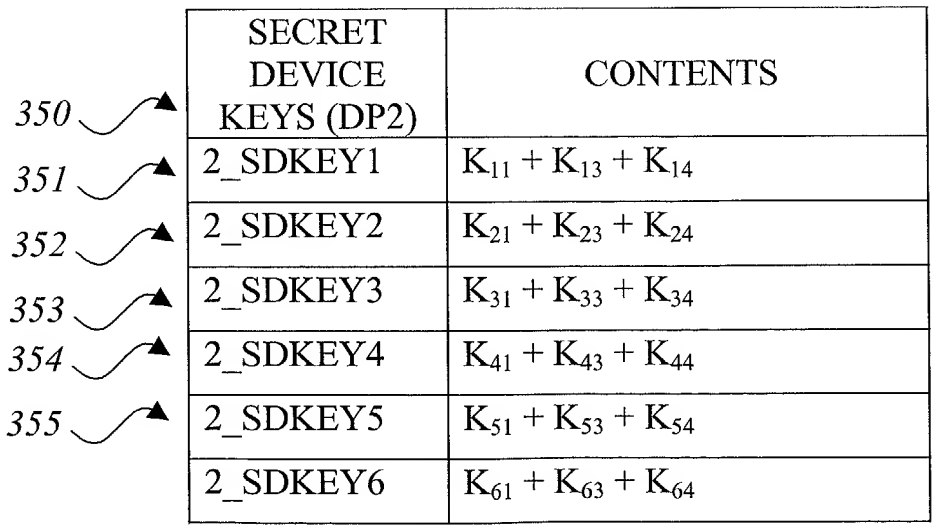

310
300
240
1
2
3
4
5
6
K11 K12 K13 K14 K15 K16
K21 K22 K23 K24 K25 K26
K31 K32 K33 K34 K35 K36
K41 K42 K43 K44 K45 K46
K51 K52 K53 K54 K55 K56
K61 K62 K63 K64 K65 K66
KSV1
1_SDKEY1
1_SDKEY2
1_SDKEY3
1_SDKEY4
1_SDKEY5
1_SDKEY6
320
330
331
332
333
334
335
TO FIRST DIGITAL PLATFORM
KSV3
2_SDKEY1
2_SDKEY2
2_SDKEY3
2_SDKEY4
2_SDKEY5
2_SDKEY6
340
350
351
352
353
354
355
TO SECOND DIGITAL PLATFORM

Figure 3



	SELECT DEVICE KEYS (DP1)	CONTENTS
330		
331	1_SDKEY1	$K_{21} + K_{31} + K_{51}$
332	1_SDKEY2	$K_{22} + K_{32} + K_{52}$
333	1_SDKEY3	$K_{23} + K_{33} + K_{53}$
334	1_SDKEY4	$K_{24} + K_{34} + K_{54}$
335	1_SDKEY5	$K_{25} + K_{35} + K_{55}$
	1_SDKEY6	$K_{26} + K_{36} + K_{56}$

Figure 4



	SECRET DEVICE KEYS (DP2)	CONTENTS
350		
351	2_SDKEY1	$K_{11} + K_{13} + K_{14}$
352	2_SDKEY2	$K_{21} + K_{23} + K_{24}$
353	2_SDKEY3	$K_{31} + K_{33} + K_{34}$
354	2_SDKEY4	$K_{41} + K_{43} + K_{44}$
355	2_SDKEY5	$K_{51} + K_{53} + K_{54}$
	2_SDKEY6	$K_{61} + K_{63} + K_{64}$

Figure 5

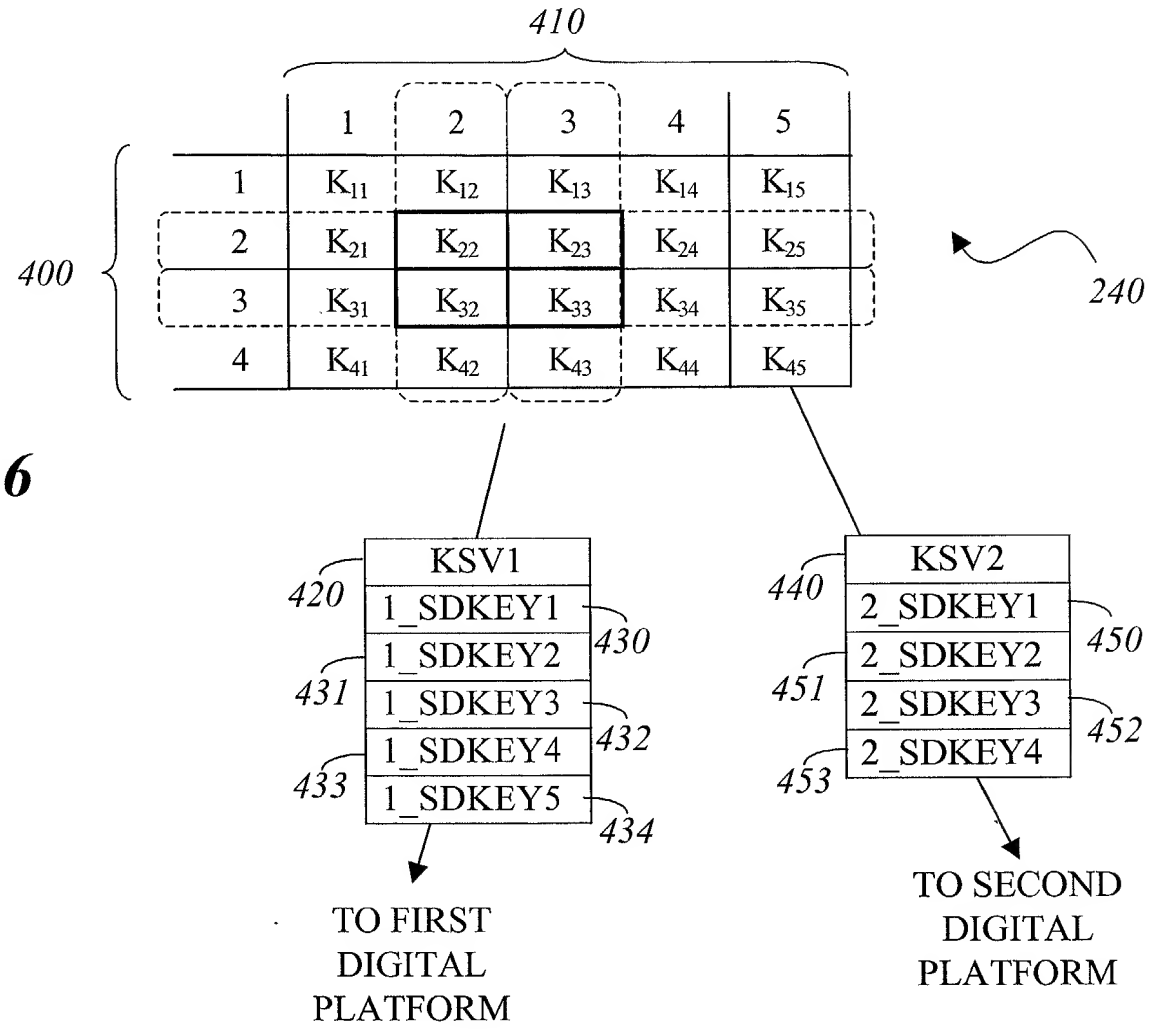

410
1
2
3
4
5
1
K11
K12
K13
K14
K15
2
K21
K22
K23
K24
K25
3
K31
K32
K33
K34
K35
4
K41
K42
K43
K44
K45
400
240
KSV1
420
1_SDKEY1
430
1_SDKEY2
431
1_SDKEY3
432
1_SDKEY4
433
1_SDKEY5
434
TO FIRST DIGITAL PLATFORM
KSV2
440
2_SDKEY1
450
2_SDKEY2
451
2_SDKEY3
452
2_SDKEY4
453
TO SECOND DIGITAL PLATFORM

Figure 6

	SECRET DEVICE KEYS (DP1)	CONTENTS
430	1_SDKEY1	$K_{21} + K_{31}$
431	1_SDKEY2	$K_{22} + K_{32}$
432	1_SDKEY3	$K_{23} + K_{33}$
433	1_SDKEY4	$K_{24} + K_{34}$
434	1_SDKEY5	$K_{25} + K_{35}$

Figure 7

	SECRET DEVICE KEYS (DP2)	CONTENTS
450	2_SDKEY1	$K_{12} + K_{13}$
451	2_SDKEY2	$K_{22} + K_{23}$
452	2_SDKEY3	$K_{32} + K_{33}$
453	2_SDKEY4	$K_{42} + K_{43}$

Figure 8

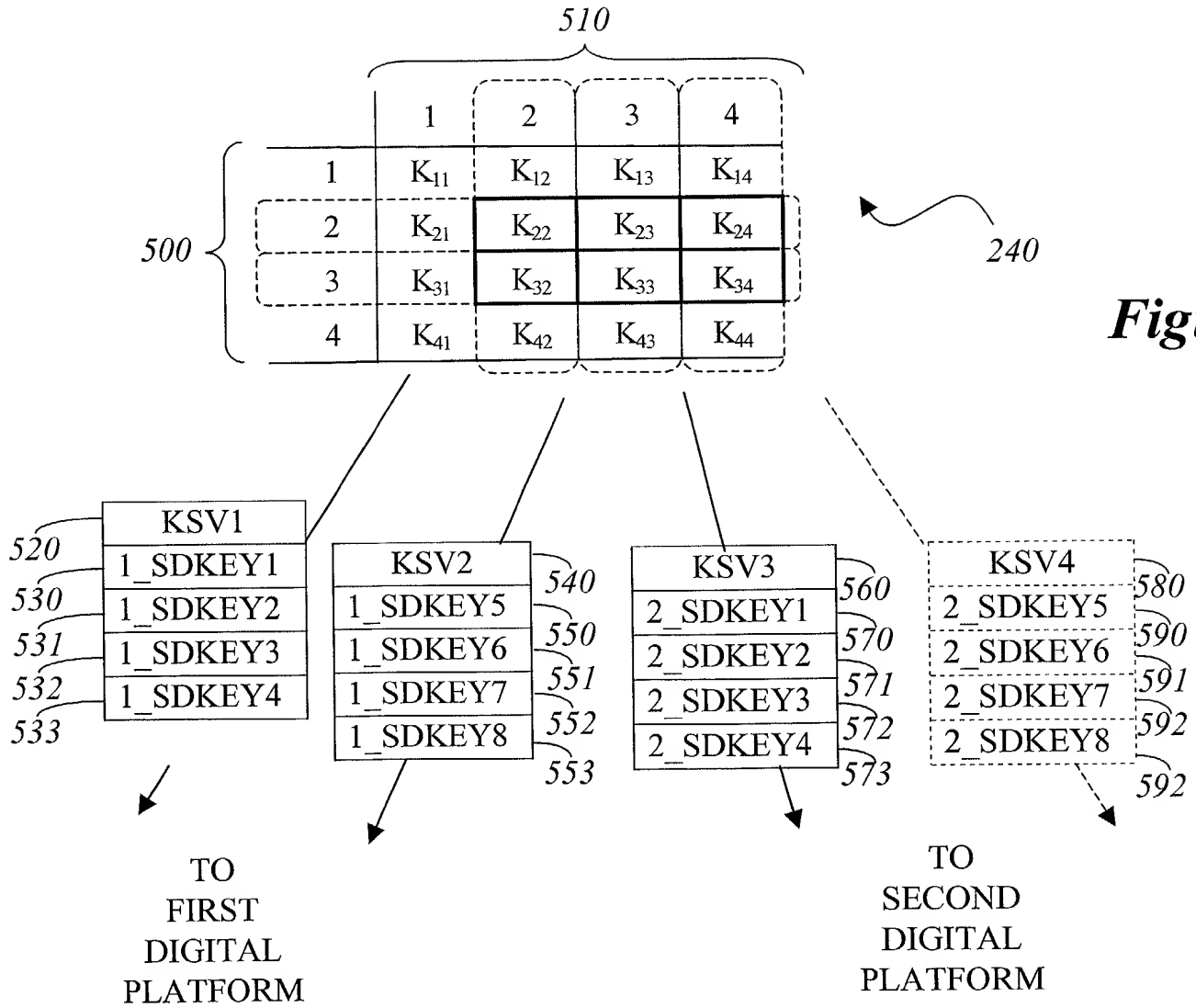

510
500
240
1
2
3
4
K11
K12
K13
K14
K21
K22
K23
K24
K31
K32
K33
K34
K41
K42
K43
K44
KSV1
1_SDKEY1
1_SDKEY2
1_SDKEY3
1_SDKEY4
520
530
531
532
533
KSV2
1_SDKEY5
1_SDKEY6
1_SDKEY7
1_SDKEY8
540
550
551
552
553
KSV3
2_SDKEY1
2_SDKEY2
2_SDKEY3
2_SDKEY4
560
570
571
572
573
KSV4
2_SDKEY5
2_SDKEY6
2_SDKEY7
2_SDKEY8
580
590
591
592
592
TO FIRST DIGITAL PLATFORM
TO SECOND DIGITAL PLATFORM

Figure 9

	SECRET DEVICE KEYS (DP1)	CONTENTS
530		
531	1_SDKEY1	$K_{21} + K_{31}$
532	1_SDKEY2	$K_{22} + K_{32}$
533	1_SDKEY3	$K_{23} + K_{33}$
	1_SDKEY4	$K_{24} + K_{34}$

Figure 10

	SECRET DEVICE KEYS (DP2)	CONTENTS
550		
551	1_SDKEY5	$K_{12} + K_{14}$
552	1_SDKEY6	$K_{22} + K_{24}$
553	1_SDKEY7	$K_{32} + K_{34}$
	1_SDKEY8	$K_{42} + K_{44}$

Figure 11

	SECRET DEVICE KEYS (DP1)	CONTENTS
570		
571	2_SDKEY1	$K_{12} + K_{13}$
572	2_SDKEY2	$K_{22} + K_{23}$
573	2_SDKEY3	$K_{32} + K_{33}$
	2_SDKEY4	$K_{42} + K_{43}$

Figure 12

	SECRET DEVICE KEYS (DP2)	CONTENTS
590		
591	2_SDKEY5	$K_{21} + K_{31}$
592	2_SDKEY6	$K_{22} + K_{32}$
593	2_SDKEY7	$K_{23} + K_{33}$
	2_SDKEY8	$K_{24} + K_{34}$

Figure 13

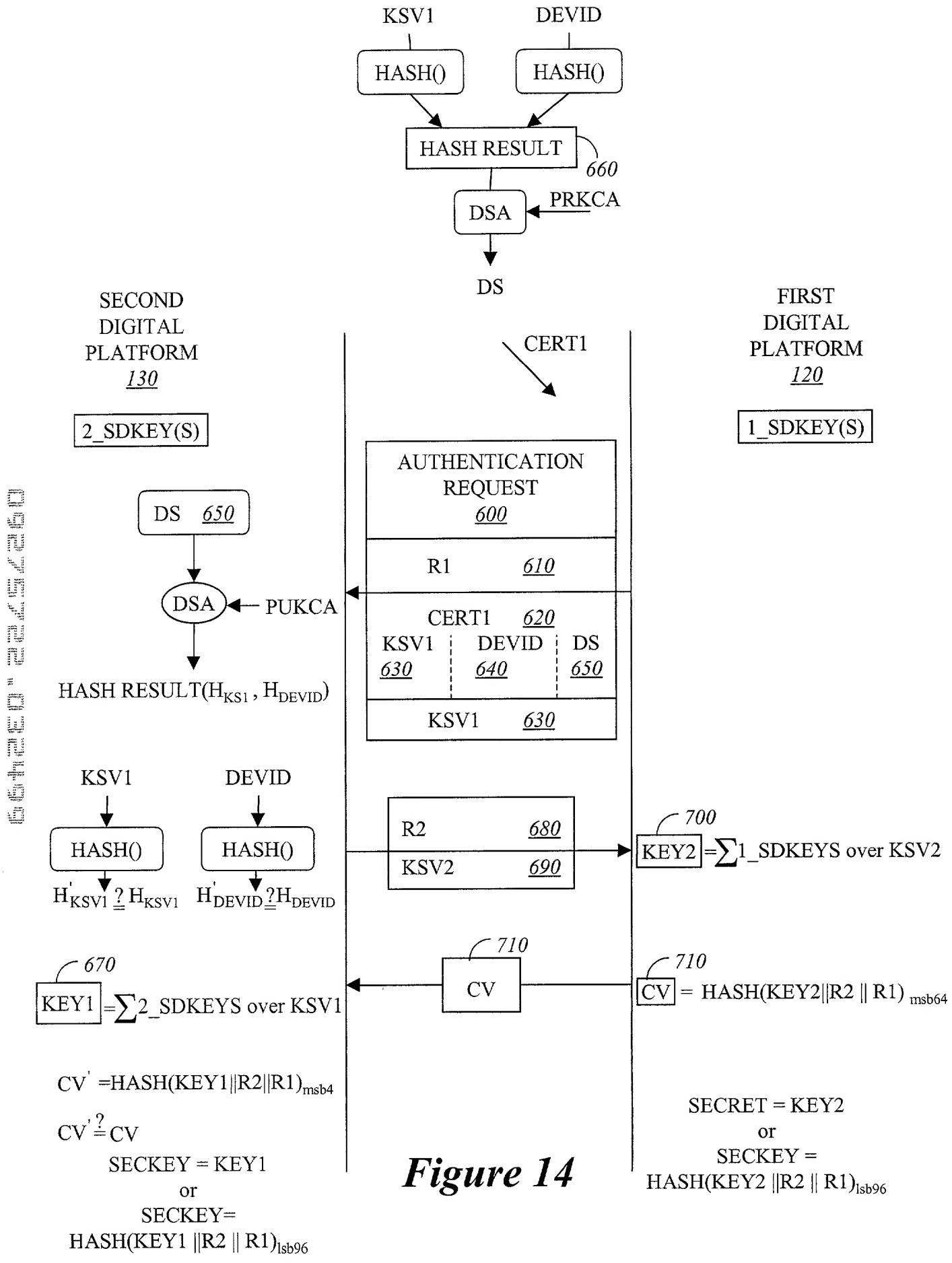

KSV1
DEVID
HASH()
HASH()
HASH RESULT
660
DSA
PRKCA
DS
SECOND DIGITAL PLATFORM
130
FIRST DIGITAL PLATFORM
120
CERT1
2_SDKEY(S)
1_SDKEY(S)
AUTHENTICATION REQUEST
600
R1
610
CERT1
620
KSV1
630
DEVID
640
DS
650
KSV1
630
DS
650
DSA
PUKCA
HASH RESULT(H_{KS1}, H_{DEVID})
KSV1
DEVID
HASH()
HASH()
$H'_{KSV1} \stackrel{?}{=} H_{KSV1}$
$H'_{DEVID} \stackrel{?}{=} H_{DEVID}$
R2
680
KSV2
690
700
KEY2 $=\sum$1_SDKEYS over KSV2
710
CV
710
CV = HASH(KEY2||R2 || R1) msb64
670
KEY1 $=\sum$2_SDKEYS over KSV1
$CV' = HASH(KEY1||R2||R1)_{msb4}$
$CV' \stackrel{?}{=} CV$
SECKEY = KEY1
or
SECKEY= HASH(KEY1 ||R2 || R1)$_{lsb96}$
SECRET = KEY2
or
SECKEY = HASH(KEY2 ||R2 || R1)$_{lsb96}$

Figure 14

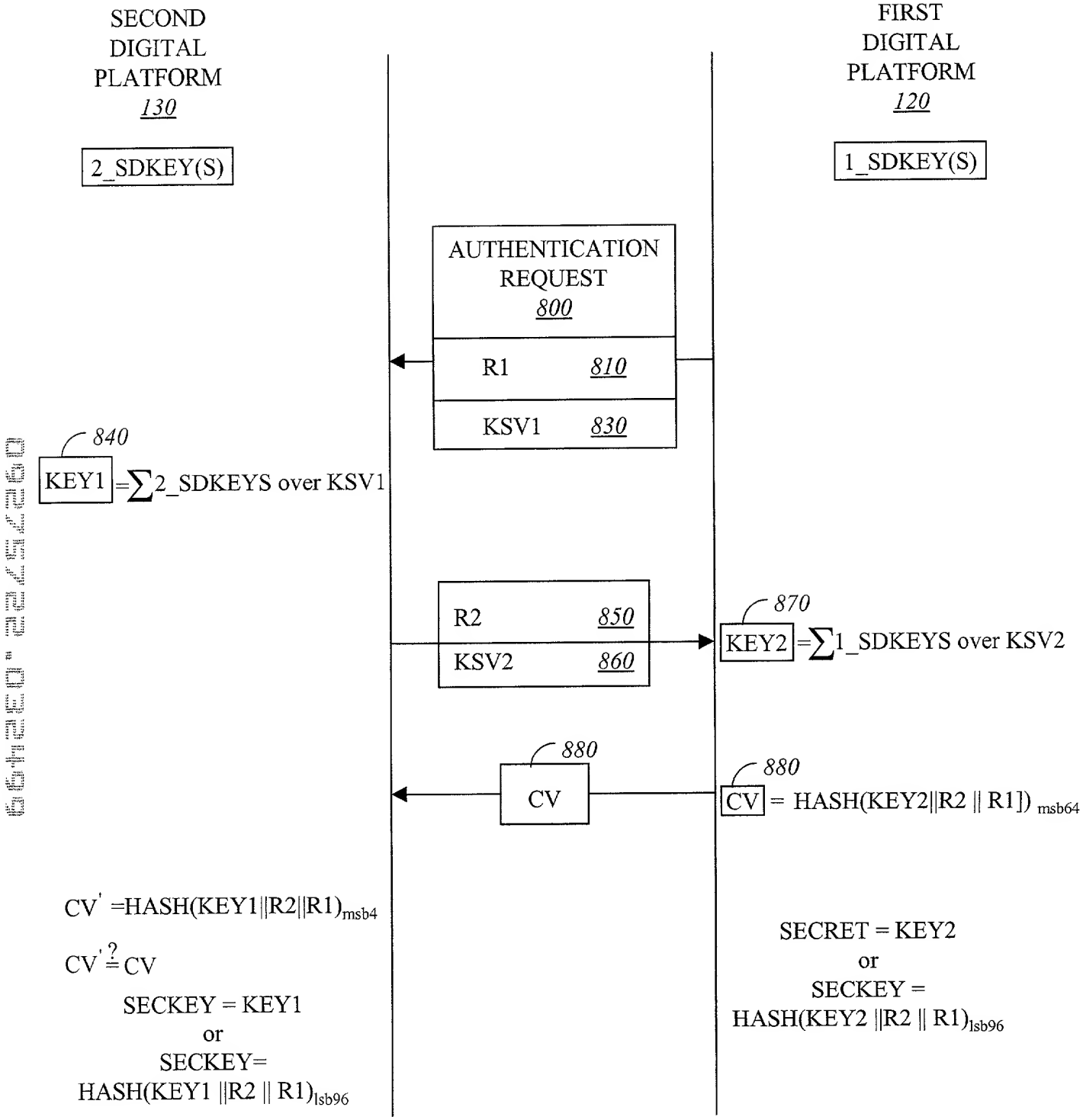

SECOND DIGITAL PLATFORM 130
2_SDKEY(S)
FIRST DIGITAL PLATFORM 120
1_SDKEY(S)
AUTHENTICATION REQUEST 800
R1 810
KSV1 830
840
KEY1 =∑2_SDKEYS over KSV1
R2 850
KSV2 860
870
KEY2 =∑1_SDKEYS over KSV2
880
CV
880
CV = HASH(KEY2||R2 || R1])msb64
CV' =HASH(KEY1||R2||R1)msb4
CV' ? CV
SECKEY = KEY1
or
SECKEY=
HASH(KEY1 ||R2 || R1)lsb96
SECRET = KEY2
or
SECKEY =
HASH(KEY2 ||R2 || R1)lsb96

Figure 15

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION (FOR INTEL CORPORATION PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

A Method and Apparatus for the Generation of Cryptographic Keys

the specification of which

[X] is attached hereto.
[ ] was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____ .
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

APPLICATION NUMBER	COUNTRY (OR INDICATE IF PCT)	DATE OF FILING (day, **month**, year)	PRIORITY CLAIMED UNDER 37 USC 119
			☐ No ☐ Yes
			☐ No ☐ Yes
			☐ No ☐ Yes

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

APPLICATION NUMBER	FILING DATE

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION NUMBER	FILING DATE	STATUS (ISSUED, PENDING, ABANDONED)

I hereby appoint BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, a firm including: William E. Alford, Reg. No. 37,764; Farzad E. Amini, 42,261; Amy M. Armstrong, P 42,265; Aloysius T. AuYeung, 35,432; W. Thomas Babbitt, 39,591; Carol F. Barry, 41,600; Jordan M. Becker, 39,602; Bradley J. Bereznak, 33,474; Michael A. Bernadicou, 35,934; Roger W. Blakely, Jr., 25,831; Gregory D. Caldwell, 39,926; Kent M. Chen, 39,630; Lawrence M. Cho, 39,942; Yongsuck Choi, 43,324; Thomas M. Coester, 39,637; Roland B. Cortes, 39,152; Barbara B. Courtney, P 42,442; Michael A. DeSanctis, 39,957; Daniel M. DeVos, 37,813; Robert A. Diehl, P 40,992; Tarek N. Fahmi, 41,402; James Y. Go, 40,621; Richard L. Gregory, Jr., P 42,607; Dinu Gruia, P 42,996; David R. Halvorson, 33,395; Thomas A. Hassing, 36,159; James A. Henry (patent agent), 41,064; Willmore F. Holbrow III, 41,845; George W. Hoover, 32,992; Eric S. Hyman, 30,139; Dag H. Johansen, 36,172; William W. Kidd, 31,772; Michael J. Mallie, 36,591; Paul A. Mendonsa, P 42,879; Darren J. Milliken, P 42,004; Thinh V. Nguyen, 42,034; Kimberley G. Nobles, 38,255; Michael A. Proksch, P 43,021; Babak Redjaian, 42,096; James H. Salter, 35,668; William W. Schaal, 39,018; James C. Scheller , 31,195; Anand Sethuraman, 43,351; Charles E. Shemwell, 40,171; Maria E. Sobrino, 31,639; Stanley W. Sokoloff, 25,128; Allan T. Sponseller, 38,318; Judith A. Szepesi, 39,393; Vincent P. Tassinari, 42,179; Edwin H. Taylor, 25,129; George G. C. Tseng, 41,355; Lester J. Vincent, 31,460; John P. Ward, 40,216; Stephen Warhola, P 43,237; Charles T. J. Weigell, 43,398; Ben J. Yorks, 33,609; Norman Zafman , 26,250; my attorneys; and Amy M. Armstrong, Reg. No. P42,265; Robert Andrew Diehl, Reg. No. P40,992; and Edwin A. Sloane, Reg. No. 34,728; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (714) 557-3800, and Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Sean Fitzgerald, Reg. No. 32,027; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; and Charles K. Young, Reg. No. 39,435; my patent attorneys, of INTEL CORPORATION with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to William W. Schaal, Reg. No. 39, 018, BLAKELY, SOKOLOFF, TAYLOR &
(Name of Attorney or Agent)
ZAFMAN LLP, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025 and direct telephone calls to William W. Schaal, Reg. No. 39, 018, (714) 557-3800.
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor (given name, family name) **David A. Lee**

Inventor's Signature (David A. Lee) Date 3/22/99

Residence Beaverton, Oregon USA Citizenship USA
(City , State) *(Country)*

P. O. Address 740 SW Willow Creek Drive

Beaverton, Oregon 97006 USA

Full Name of Second/Joint Inventor (given name, family name)

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City , State) *(Country)*

P. O. Address _____

_____

Full Name of Third/Joint Inventor (given name, family name)

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City , State) *(Country)*

P. O. Address _____

_____

Full Name of Fourth/Joint Inventor (given name, family name)

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City , State) *(Country)*

P. O. Address _____

_____